Sogamoso, Octubre de 2023

Ingeniero
JUAN CARLOS BERNAL MESA
Profesional Universitario
Oficina de la Tics y Comunicaciones
Alcaldía de Sogamoso

Asunto: Presentación de informe N°7 contrato 20230294

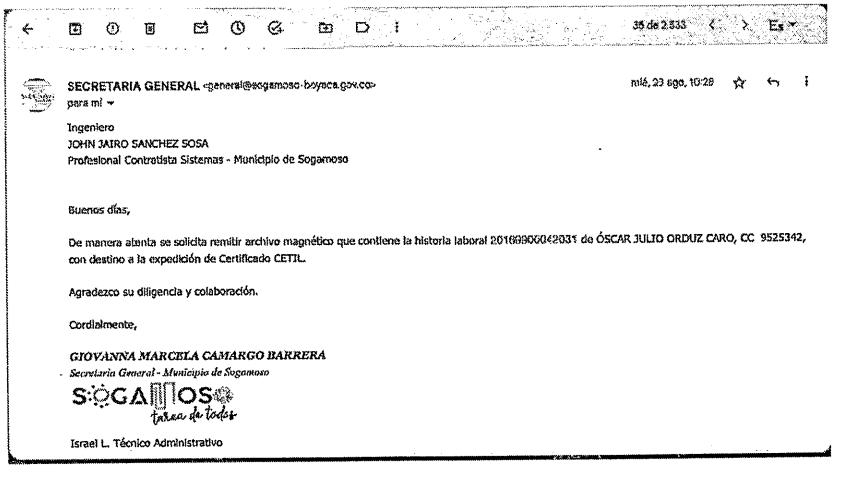
Respetado Ingeniero:

Cordialmente me permito presentar informe del periodo comprendido entre 23 de Agosto al 22 de Septiembre; teniendo en cuenta contrato de prestación de servicios de apoyo a la gestión número 20230294 así:

Actividad:

1. **Apoyar el soporte técnico de la plataforma tecnológica y redes informáticas del Municipio de Sogamoso en sus diferentes dependencias.**

- Por parte de Secretaria General se solicita por correo electrónico del dia 23 de agosto, se solicita copia de la historia laboral del funcionario ÓSCAR JULIO ORDUZ CARO el cual es consultada primeramente en el sistema Orfeo y se descarga el documento responder por el mismo medio con documento adjunto.



35 de 2.533

SECRETARIA GENERAL <general@sogamoso-boyaca.gov.co> mié, 23 ago, 10:28

para mí

Ingeniero
JOHN JAIRO SANCHEZ SOSA
Profesional Contratista Sistemas - Municipio de Sogamoso

Buenos días,

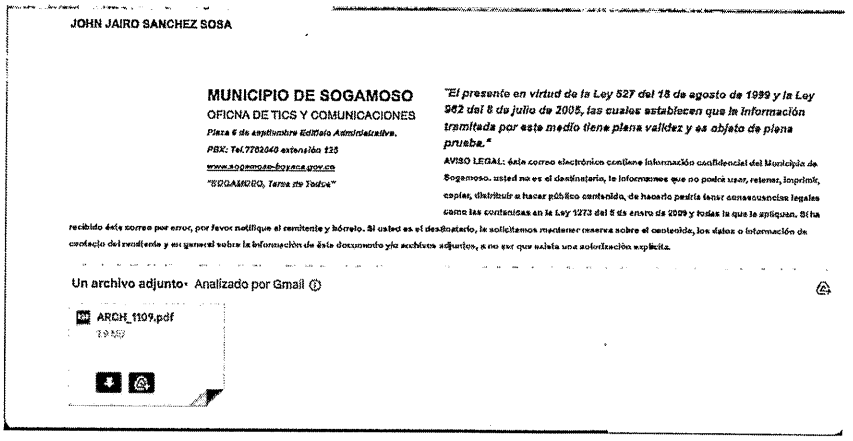
De manera atenta se solicita remitir archivo magnético que contiene la historia laboral 20166990042031 de ÓSCAR JULIO ORDUZ CARO, CC 9525342, con destino a la expedición de Certificado CETIL.

Agradezco su diligencia y colaboración.

Cordialmente,

GIOVANNA MARCELA CAMARGO BARRERA
Secretaria General - Municipio de Sogamoso
SOGAMOSO
tarea de todos

Israel L. Técnico Administrativo



JOHN JAIRO SANCHEZ SOSA

MUNICIPIO DE SOGAMOSO
OFICINA DE TICS Y COMUNICACIONES
Plaza 6 de septiembre Edificio Administrativo.
PBX: Tel:7702040 extensión 125
www.sogamoso-boyaca.gov.co
"SOGAMOSO, Tierra de Todos"

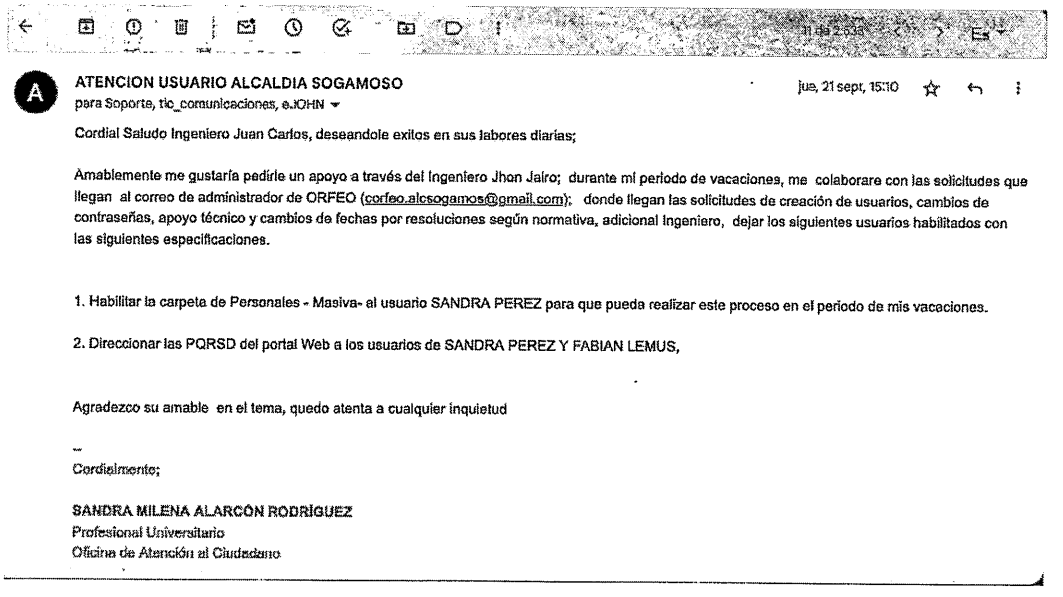
"El presente en virtud de la Ley 527 del 18 de agosto de 1999 y la Ley 962 del 8 de julio de 2005, las cuales establecen que la información tramitada por este medio tiene plena validez y es objeto de plena prueba."

AVISO LEGAL: éste correo electrónico contiene información confidencial del Municipio de Sogamoso. usted no es el destinatario, le informamos que no podrá usar, retener, imprimir, copiar, distribuir o hacer público contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas la que le apliquen. Si ha recibido éste correo por error, por favor notifique al remitente y bórrelo. Si usted es el destinatario, le solicitamos mantener reserva sobre el contenido, los datos o información de contacto del remitente y en general sobre la información de éste documento y/o archivos adjuntos, a no ser que medie una autorización explícita.

Un archivo adjunto· Analizado por Gmail

ARCH_1109.pdf

- La oficina de atención al usuario mediante correo electrónico hace la solicitud de asignación de permisos para los funcionarios SANDRA YOLIMA PEREZ Y FABIAN LEMUS para que puedan tanto realizar radicaciones masivas y recepción de PQRD desde la plataforma Orfeo. Se asignan dichos permisos desde el modulo de administración de usuarios.



A

ATENCION USUARIO ALCALDIA SOGAMOSO
para Soporte, tic_comunicaciones, e.JOHN

jue, 21 sept, 15:10

Cordial Saludo Ingeniero Juan Carlos, deseandole exitos en sus labores diarias;

Amablemente me gustaría pedirle un apoyo a través del Ingeniero Jhon Jairo; durante mi periodo de vacaciones, me colaborare con las solicitudes que llegan al correo de administrador de ORFEO (corfeo.alcsogamos@gmail.com); donde llegan las solicitudes de creación de usuarios, cambios de contraseñas, apoyo técnico y cambios de fechas por resoluciones según normativa, adicional Ingeniero, dejar los siguientes usuarios habilitados con las siguientes especificaciones.

1. Habilitar la carpeta de Personales - Masiva- al usuario SANDRA PEREZ para que pueda realizar este proceso en el periodo de mis vacaciones.

2. Direccionar las PQRSD del portal Web a los usuarios de SANDRA PEREZ Y FABIAN LEMUS,

Agradezco su amable en el tema, quedo atenta a cualquier inquietud

--
Cordialmente;

SANDRA MILENA ALARCÓN RODRÍGUEZ
Profesional Universitario
Oficina de Atención al Ciudadano

- Se hizo traslado de scanner desde el despacho del señor alcalde y se instala en equipo de la oficina jurídica realizando la configuración respectiva para escaneo de alto volumen de información dirigido a procuraduría.

- Se apoya a la oficina de sistemas en realizar seguimiento a copias de seguridad del servidor de bases de datos sysman ya que no se están

generando especialmente la de predial. Se ingresa al servidor junto con la ingeniera Nancy Álvarez validando de primera mano la configuración de la tarea de copias. Se realizo una reprogramación de esta para solventar el problema.

2. **Realizar el análisis de tráfico y paquetes de información de entrada y salida de la red de datos de la administración municipal, reportando a la entidad de manera oportuna, anomalías o incidentes de ciberseguridad según el procedimiento de seguridad y privacidad de la información del municipio de Sogamoso.**

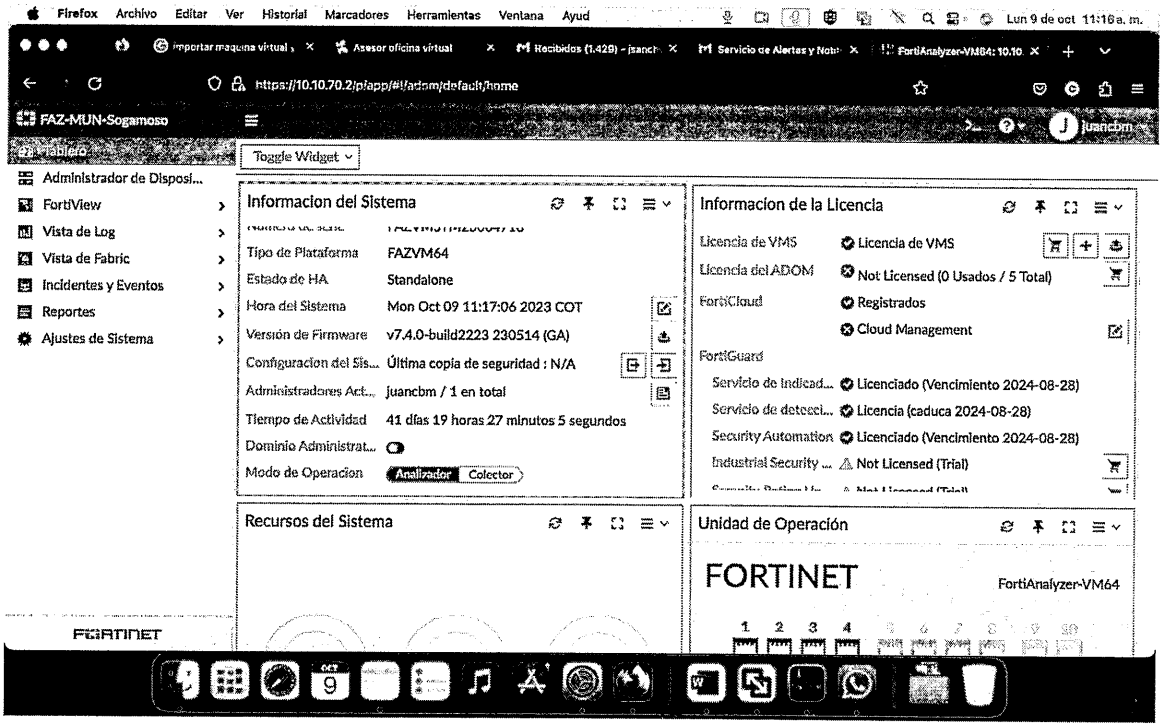
Para este periodo se recibe capacitación por parte de Fortinet en uso y apropiación de la herramienta fortianalyzer, el cual recopila y analiza los logs que se generan en los cuatros Fortinet que tiene la administración municipal (torre 6, pintor, edificio rojas y sec educación), este análisis es clasificado en módulos de seguridad que reportan que casos de atraque o intento de ingreso no autorizado ya sea por hacker u virus.

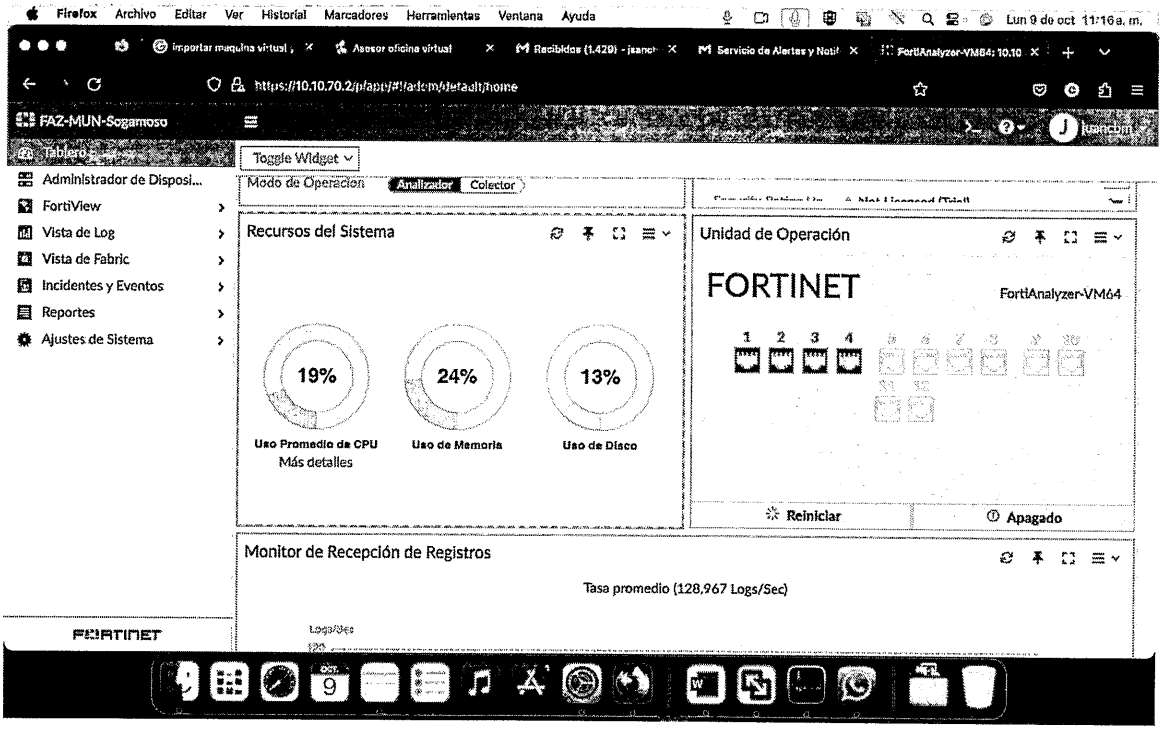
Estos reportes deben ser analizados constantemente ya que parten desde los mismos logs y de forma manual, para aquellos que no se han podido resolver, se ingresa al Fortinet para realizar acciones respectivas como creación de políticas o limitaciones de acceso.

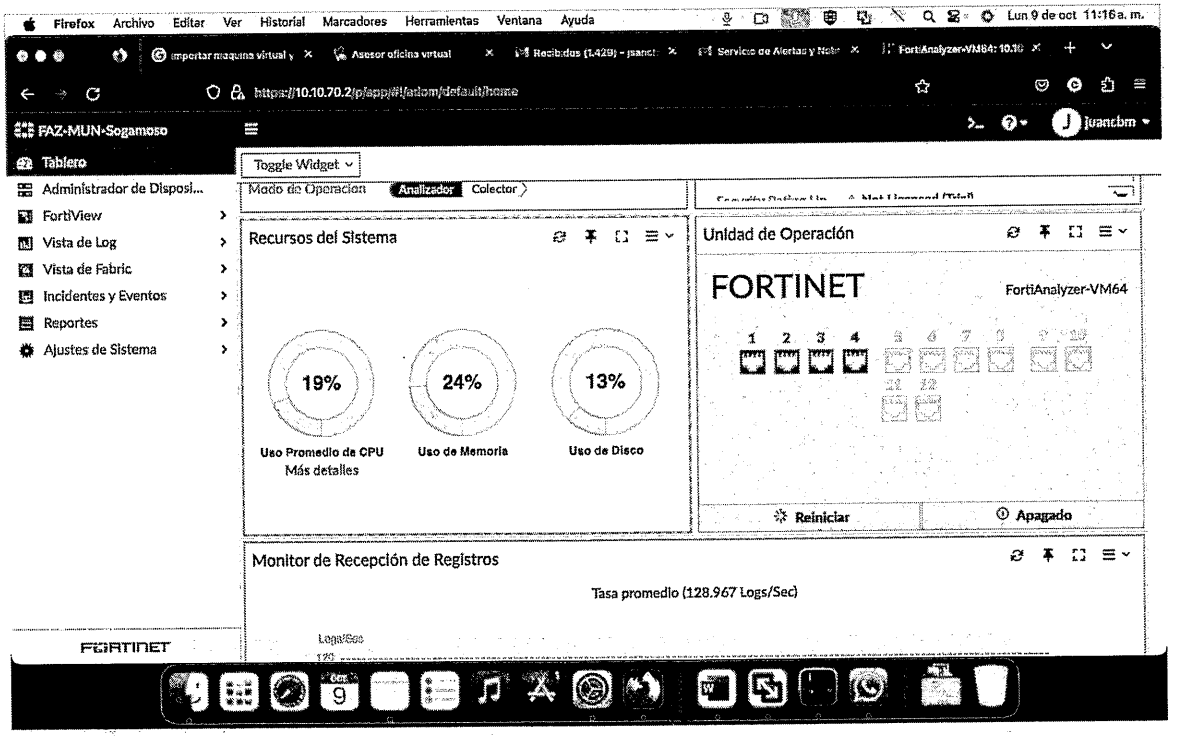
Para este periodo de entrenamiento se detecta una serie de intentos de hackeo por un herramienta TeamViewer el cual está instalada en un servidor de planeación.

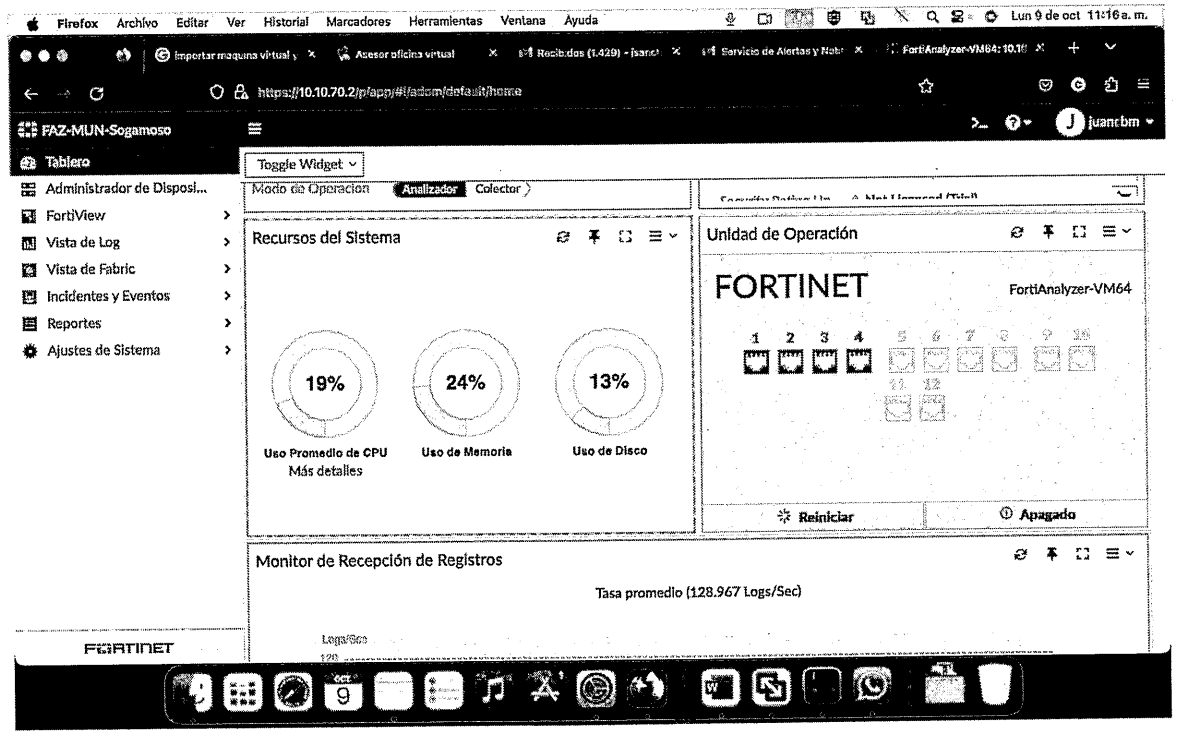
Se revisa el servidor y se realiza la desinstalación del aplicativo para reducir el nivel de advertencia y se insta al funcionario a cargo del al maquina a reportar en la oficina de sistemas la necesitad de validar la instalación o concesión de acceso por este tipo de herramientas.

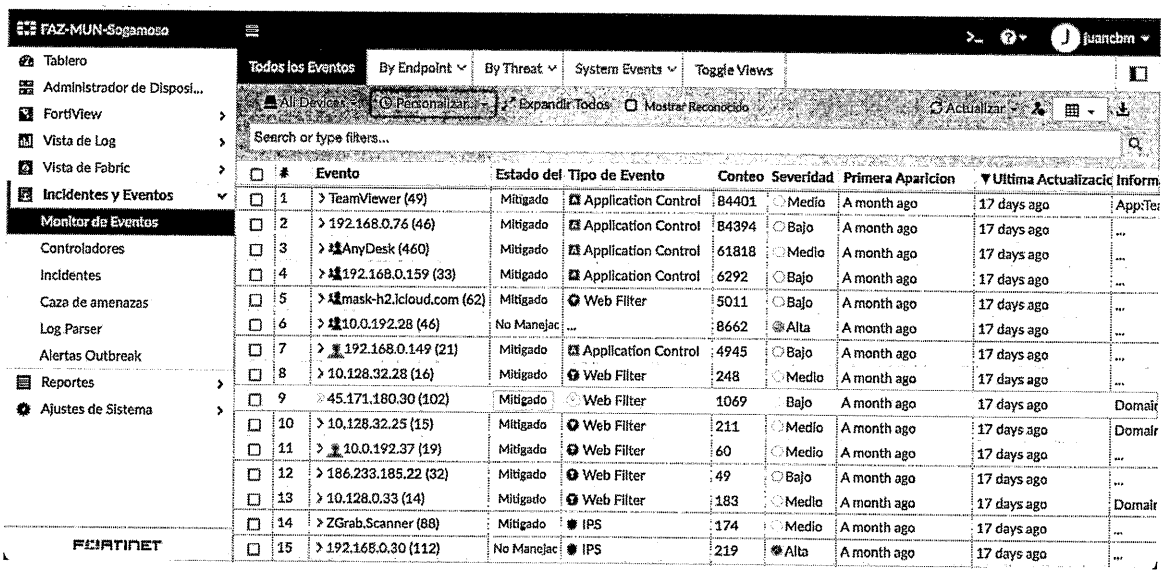
De igual forma se han evidenciado otro tipo de ingresos a paginas baneadas por los filtros de Fortinet y ha referenciado niveles altos en criticidad y vulnerabilidad. Dichas páginas se han ido ingresando de manera manual a la política de restricción de página del Fortinet.

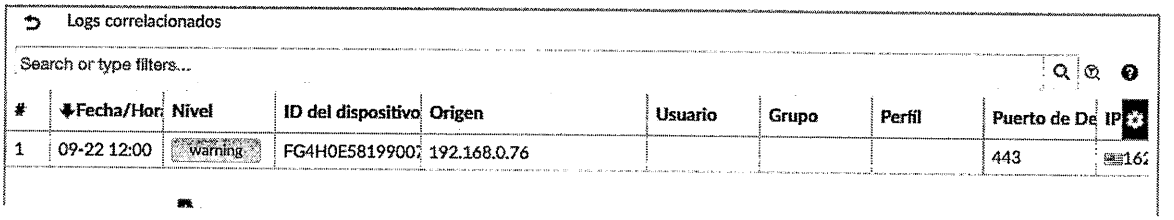

FAZ-MUN-Sogamoso
Toggle Widget
Administrador de Disposi...
FortiView
Vista de Log
Vista de Fabric
Incidentes y Eventos
Reportes
Ajustes de Sistema
Informacion del Sistema
Tipo de Plataforma FAZVM64
Estado de HA Standalone
Hora del Sistema Mon Oct 09 11:17:06 2023 COT
Versión de Firmware v7.4.0-build2223 230514 (GA)
Configuracion del Sis... Última copia de seguridad : N/A
Administradores Act... juancbm / 1 en total
Tiempo de Actividad 41 días 19 horas 27 minutos 5 segundos
Dominio Administrat...
Modo de Operacion Analizador Colector
Informacion de la Licencia
Licencia de VMS Licencia de VMS
Licencia del ADOM Not Licensed (0 Usados / 5 Total)
FortiCloud Registrados
Cloud Management
FortiGuard
Servicio de Indicad... Licenciado (Vencimiento 2024-08-28)
Servicio de detecci... Licencia (caduca 2024-08-28)
Security Automation Licenciado (Vencimiento 2024-08-28)
Industrial Security ... Not Licensed (Trial)
Recursos del Sistema
Unidad de Operación
FORTINET
FortiAnalyzer-VM64
1 2 3 4

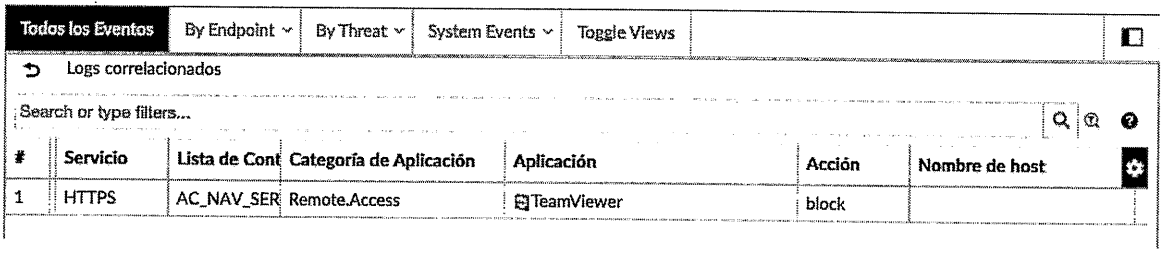

FAZ-MUN-Sogamoso
Toggle Widget
Administrador de Disposi...
FortiView
Vista de Log
Vista de Fabric
Incidentes y Eventos
Reportes
Ajustes de Sistema
Modo de Operacion Analizador Colector
Recursos del Sistema
19%
Uso Promedio de CPU
Más detalles
24%
Uso de Memoria
13%
Uso de Disco
Unidad de Operación
FORTINET
FortiAnalyzer-VM64
1 2 3 4
Reiniciar
Apagado
Monitor de Recepción de Registros
Tasa promedio (128,967 Logs/Sec)

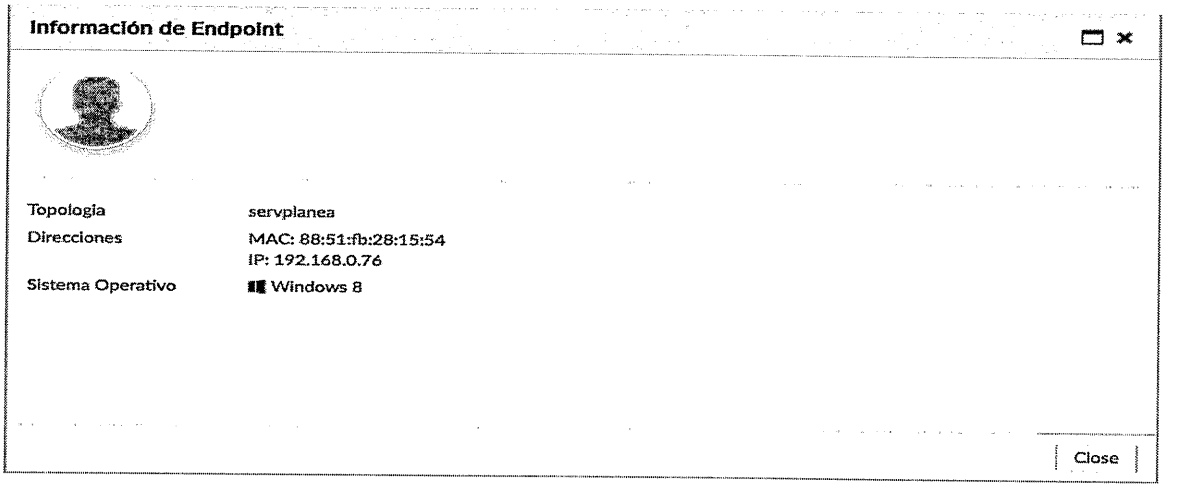

Firefox Archivo Editar Ver Historial Marcadores Herramientas Ventana Ayuda
Lun 9 de oct 11:16 a. m.
https://10.10.70.2/p/app/#/adom/default/home
FAZ-MUN-Sogamoso
juanebm
Tablero
Administrador de Disposi...
FortiView
Vista de Log
Vista de Fabric
Incidentes y Eventos
Reportes
Ajustes de Sistema
Toggle Widget
Modo de Operación
Analizador
Colector
Recursos del Sistema
19%
Uso Promedio de CPU
Más detalles
24%
Uso de Memoria
13%
Uso de Disco
Unidad de Operación
FORTINET
FortiAnalyzer-VM64
Reiniciar
Apagado
Monitor de Recepción de Registros
Tasa promedio (128.967 Logs/Sec)
FORTINET


Firefox Archivo Editar Ver Historial Marcadores Herramientas Ventana Ayuda
Lun 9 de oct 11:16 a. m.
https://10.10.70.2/p/app/#/adom/default/home
FAZ-MUN-Sogamoso
juanebm
Tablero
Administrador de Disposi...
FortiView
Vista de Log
Vista de Fabric
Incidentes y Eventos
Reportes
Ajustes de Sistema
Toggle Widget
Modo de Operación
Analizador
Colector
Recursos del Sistema
19%
Uso Promedio de CPU
Más detalles
24%
Uso de Memoria
13%
Uso de Disco
Unidad de Operación
FORTINET
FortiAnalyzer-VM64
Reiniciar
Apagado
Monitor de Recepción de Registros
Tasa promedio (128.967 Logs/Sec)
FORTINET


FAZ-MUN-Sogamoso
juanchm
Tablero
Administrador de Disposi...
FortiView
Vista de Log
Vista de Fabric
Incidentes y Eventos
Monitor de Eventos
Controladores
Incidentes
Caza de amenazas
Log Parser
Alertas Outbreak
Reportes
Ajustes de Sistema
FORTINET
Todos los Eventos
By Endpoint
By Threat
System Events
Toggle Views
All Devices
Personalizar...
Expandir Todos
Mostrar Reconocido
Actualizar
Search or type filters...
Evento Estado del Tipo de Evento Conteo Severidad Primera Aparicion ▼Ultima Actualizacic Inform
1 TeamViewer (49) Mitigado Application Control 84401 Medio A month ago 17 days ago
2 192.168.0.76 (46) Mitigado Application Control 84394 Bajo A month ago 17 days ago
3 AnyDesk (460) Mitigado Application Control 61818 Medio A month ago 17 days ago
4 192.168.0.159 (33) Mitigado Application Control 6292 Bajo A month ago 17 days ago
5 mask-h2.icloud.com (62) Mitigado Web Filter 5011 Bajo A month ago 17 days ago
6 10.0.192.28 (46) No Manejac ... 8662 Alta A month ago 17 days ago
7 192.168.0.149 (21) Mitigado Application Control 4945 Bajo A month ago 17 days ago
8 10.128.32.28 (16) Mitigado Web Filter 248 Medio A month ago 17 days ago
9 45.171.180.30 (102) Mitigado Web Filter 1069 Bajo A month ago 17 days ago Domair
10 10.128.32.25 (15) Mitigado Web Filter 211 Medio A month ago 17 days ago Domair
11 10.0.192.37 (19) Mitigado Web Filter 60 Medio A month ago 17 days ago
12 186.233.185.22 (32) Mitigado Web Filter 49 Bajo A month ago 17 days ago
13 10.128.0.33 (14) Mitigado Web Filter 183 Medio A month ago 17 days ago Domair
14 ZGrab.Scanner (88) Mitigado IPS 174 Medio A month ago 17 days ago
15 192.168.0.30 (112) No Manejac IPS 219 Alta A month ago 17 days ago

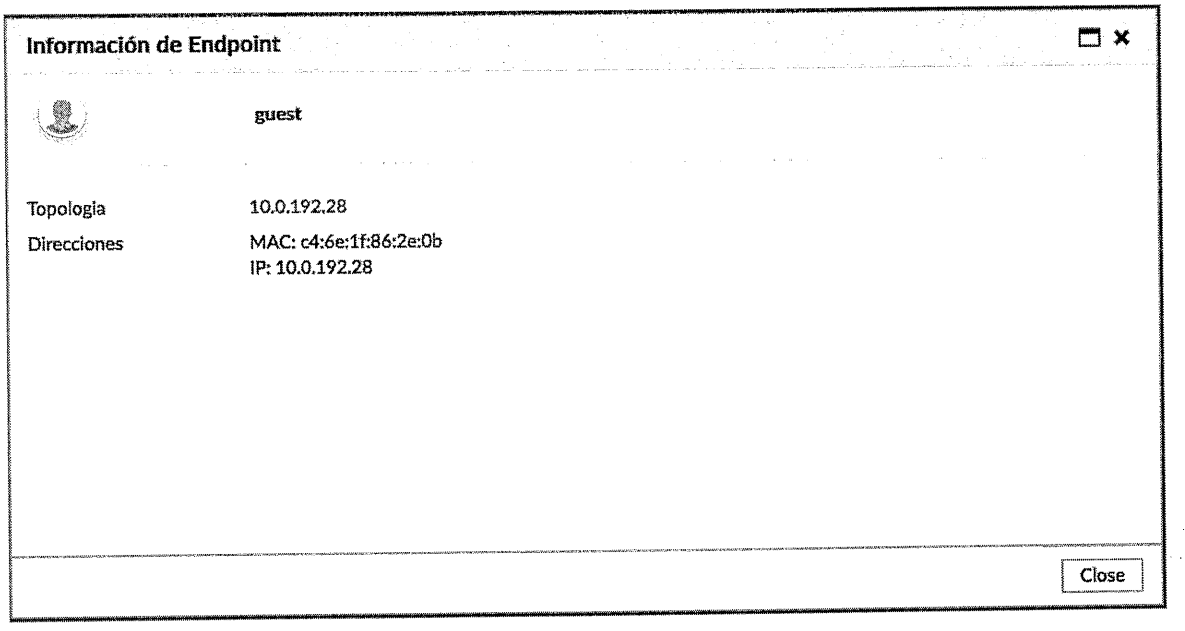

Logs correlacionados
Search or type filters...
Fecha/Hor Nivel ID del dispositivo Origen Usuario Grupo Perfil Puerto de De IP
1 09-22 12:00 warning FG4H0E5819900 192.168.0.76 443


Todos los Eventos
By Endpoint
By Threat
System Events
Toggle Views
Logs correlacionados
Search or type filters...
Servicio Lista de Cont Categoría de Aplicación Aplicación Acción Nombre de host
1 HTTPS AC_NAV_SER Remote.Access TeamViewer block


Información de Endpoint
Topología servplanea
Direcciones MAC: 88:51:fb:28:15:54
IP: 192.168.0.76
Sistema Operativo Windows 8
Close

Por otro lado, se detecta un intento de intrusión por puerto 64293 desde un equipo invitado que se conecta a torre 6 hacia una url externa. Esto se debe a ingreso a una pagina baneada o virus residente en el equipo el cual usa ese puerto de comunicación para envió de datos. Fortinet bloquea ese intento, pero deja la huella para realizar seguimiento.

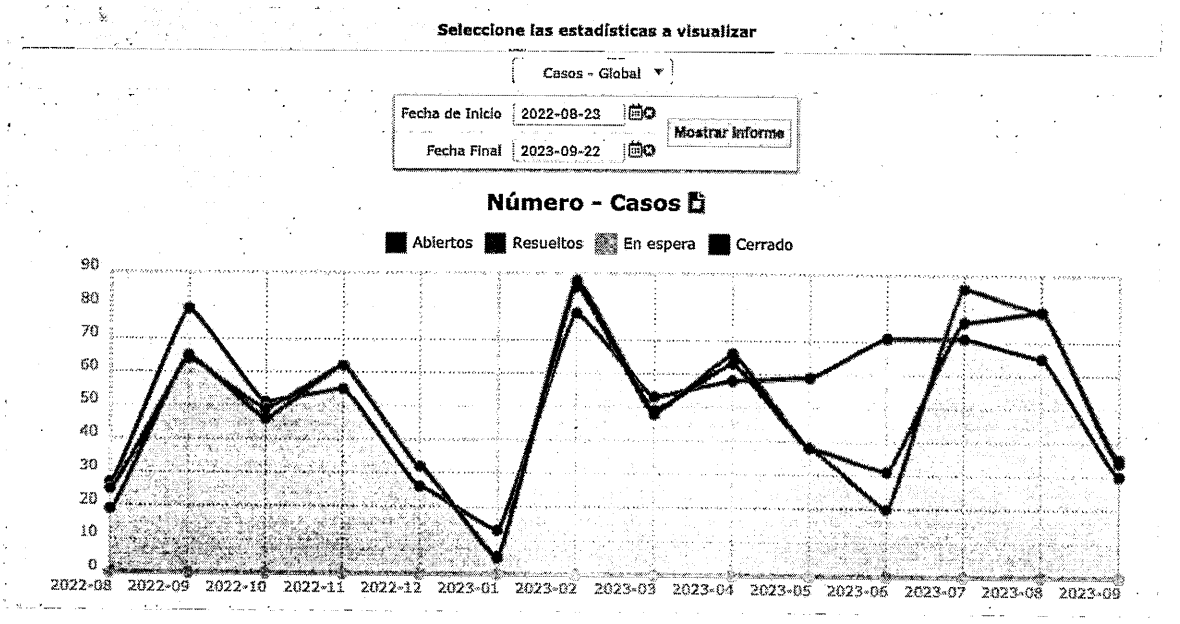
Evento	Estado del	Tipo de Evento	Conteo	Severidad	Primera Aparicion	▼Ultima Actualizacic	Información Adicic
Web request to Unrate...	Mitigado	Web Filter	1	Medio	2023-09-22 09:10:...	2023-09-22 09:10:...	Domain:186.233.18
Web request to Proxy ...	Mitigado	Web Filter	54	Medio	2023-09-21 09:21:...	2023-09-21 16:43:...	Domain:doh.dns.ap
Web request to Unrate...	Mitigado	Web Filter	15	Medio	2023-09-21 08:27:...	2023-09-21 16:22:...	Domain:186.233.18
Risky App BitTorrent bl...	Mitigado	Application Control	19	Bajo	2023-09-21 11:11:...	2023-09-21 12:31:...	AppID:6 from Cate
Risky App BitTorrent bl...	Mitigado	Application Control	874	Bajo	2023-09-20 14:19:...	2023-09-20 17:40:...	AppID:6 from Cate
Web request to Unrate...	Mitigado	Web Filter	22	Medio	2023-09-20 08:13:...	2023-09-20 17:39:...	Domain:64.31.17.5
Risky App RDP blocked	Mitigado	Application Control	26	Bajo	2023-09-20 08:36:...	2023-09-20 17:21:...	AppID:15511 from
Web request to Proxy ...	Mitigado	Web Filter	20	Medio	2023-09-20 08:06:...	2023-09-20 16:11:...	Domain:mask-h2.icl
Intrusion TCP.Split.Han...	Mitigado	IPS	1	Alta	2023-09-20 09:06:...	2023-09-20 09:06:...	outgoing intrusion,
Web request to Proxy ...	Mitigado	Web Filter	204	Medio	2023-09-19 08:22:...	2023-09-19 16:50:...	Domain:doh.dns.ap
Web request to Unrate...	Mitigado	Web Filter	2	Medio	2023-09-19 11:13:...	2023-09-19 15:23:...	Domain:64.31.17.3
Risky App Proxy.HTTP ...	Mitigado	Application Control	2	Medio	2023-09-19 09:53:...	2023-09-19 09:53:...	AppID:107347980
Web request to Unra...	Mitigado	Web Filter	28	Medio	2023-09-18 08:53:...	2023-09-18 18:21:...	Domain:84.17.40.4
Web request to Prox...	Mitigado	Web Filter	43	Medio	2023-09-18 08:30:...	2023-09-18 18:06:...	Domain:doh.dns.ap
Web request to Unrate...	Mitigado	Web Filter	5	Medio	2023-09-15 08:53:...	2023-09-15 18:35:...	Domain:186.233.18



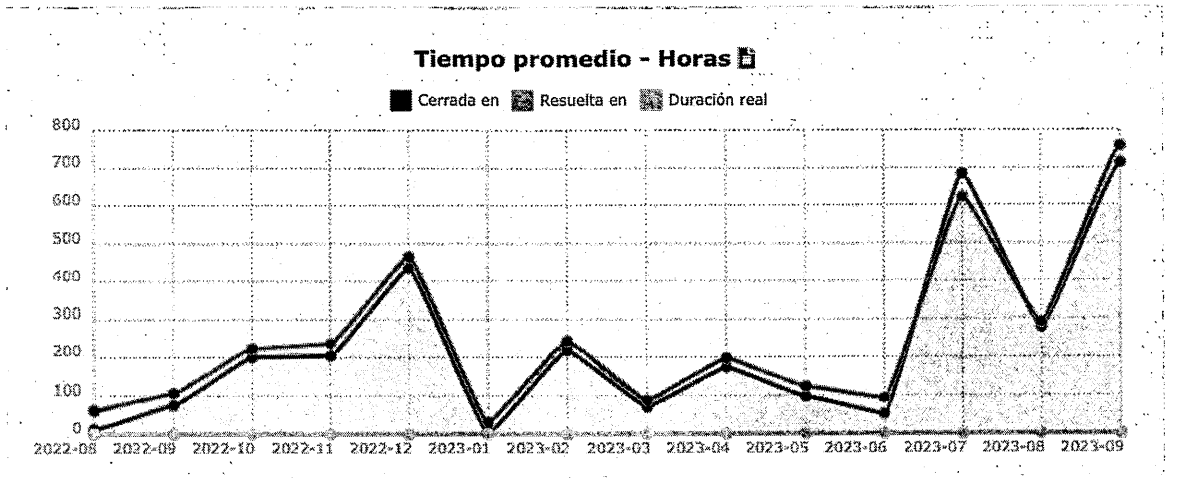
Recomendaciones: este es un trabajo de seguimiento diario donde se evidencia que la cultura del funcionario aun no es preventiva, sino que acceden sin analizar a información de dudosa procedencia y el cual es de alto nivel de contenido de virus. La recomendación es realizar un pequeño taller de uso y apropiación de normas básicas de seguridad de acceso a información, identificación de email potencialmente peligrosos.

3. **Realizar soporte técnico y gestión a la mesa de ayuda garantizando su disponibilidad e integridad de los datos para la gestión de casos del parque informático de la administración municipal.**

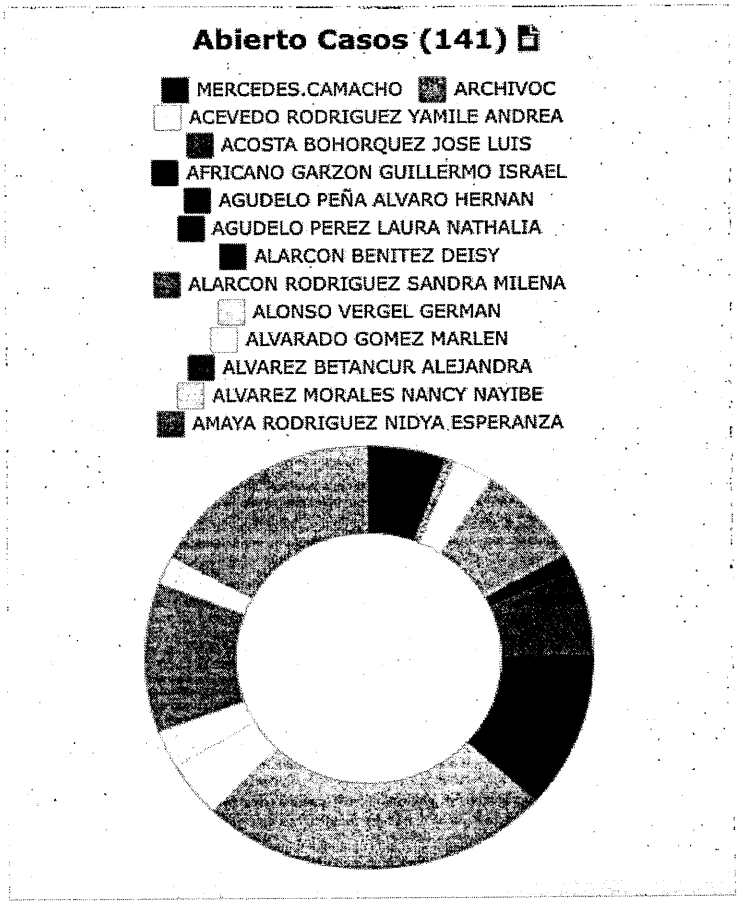
Las condiciones técnicas del aplicativo y el servidor son óptimas. Se hizo revisión previa a los casos que han sido incluidos en este nuevo periodo y se evidencia la creación de 141 casos en la administración y de esos 134 de manera oportuna se han tramitado y cerrado 135. Se puede generar la inquietud del caso de mas. Al ver la relacion de este se refleja que viene arrastrado del periodo anterior en un caso y en este se dio solucion.se conlcuye los casos generardos demuestra una efcitividad en el servicio del 95.03% para el periodo comprendido de este informe.



Esta grafica representa el numero de casos creados en sistema realizando una comprativa de estado de solicitudes.

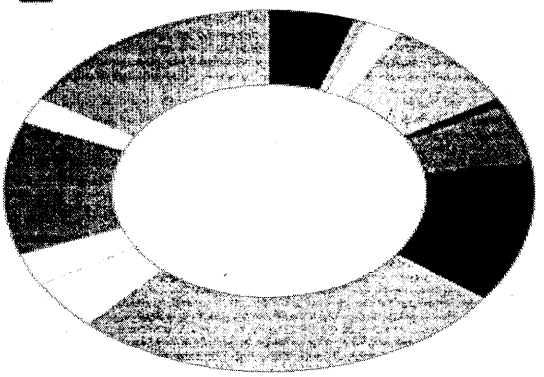


Aquí se refleja en tiempo, el promedio en atencion de un caso registrado.



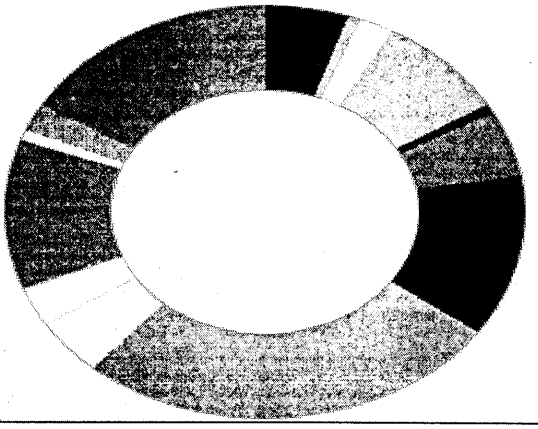
Resuelto Casos (134)

MERCEDES.CAMACHO
ARCHIVOC
ACEVEDO RODRIGUEZ YAMILE ANDREA
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ MORALES NANCY NAYIBE
AMAYA RODRIGUEZ NIDYA ESPERANZA



Cerrado Casos (135)

MERCEDES.CAMACHO
ARCHIVOC
ACEVEDO RODRIGUEZ YAMILE ANDREA
ACOSTA BOHORQUEZ JOSE LUIS
AFRICANO GARZON GUILLERMO ISRAEL
AGUDELO PEÑA ALVARO HERNAN
AGUDELO PEREZ LAURA NATHALIA
ALARCON BENITEZ DEISY
ALARCON RODRIGUEZ SANDRA MILENA
ALONSO VERGEL GERMAN
ALVARADO GOMEZ MARLEN
ALVAREZ BETANCUR ALEJANDRA
ALVAREZ GUTIERREZ YASMID ROCIO
ALVAREZ MORALES NANCY NAYIBE
AMAYA RODRIGUEZ NIDYA ESPERANZA

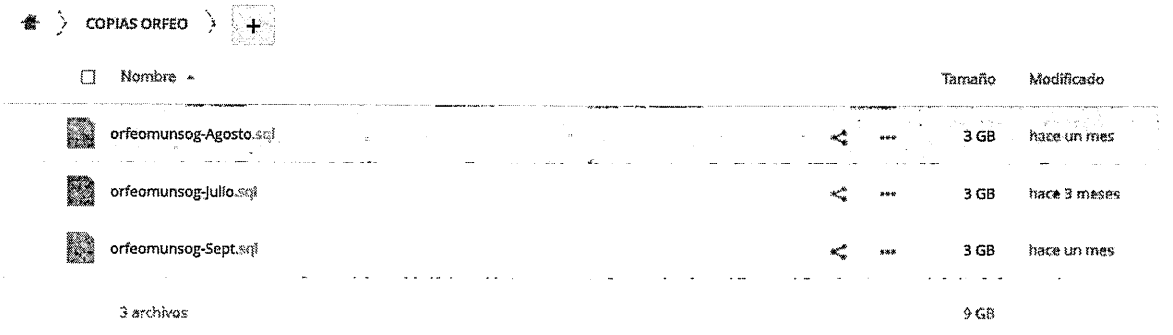


4. Realizar actualizaciones en capacitaciones en la oficina de atención al usuario relacionadas con el centro de relevo y/o demás herramientas tecnológicas dispuestas para discapacidad.

Se hace revisión en sitio del equipo donde se encuentra instalado la herramienta ZOOMTEXT para validar su funcionamiento y estado de actualizaciones para generar citación a capacitación dudas e inquietudes respecto a la herramienta. Se evidencia que la solución esta actualizada debidamente y el sistema operativo residente está en buen funcionamiento.

5. Generar copias de seguridad del software de gestión documental Orfeo que permitan su adecuado restablecimiento.

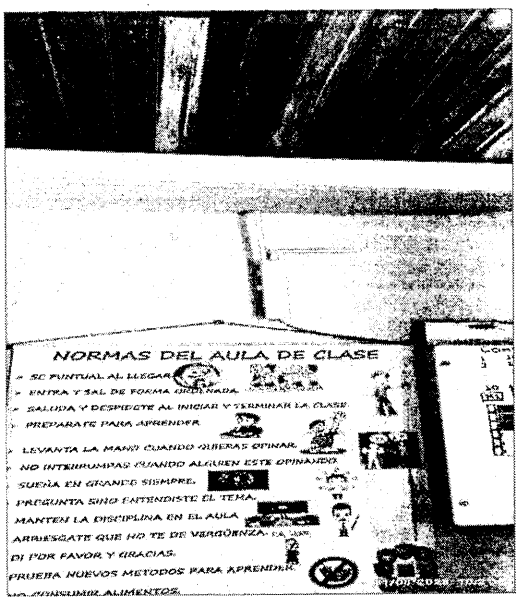
Se generan copias de seguridad correspondientes al mes de agosto – septiembre de la base de datos del sistema de gestión documental orfeo dejándolas almacenadas en la plataforma owncloud.

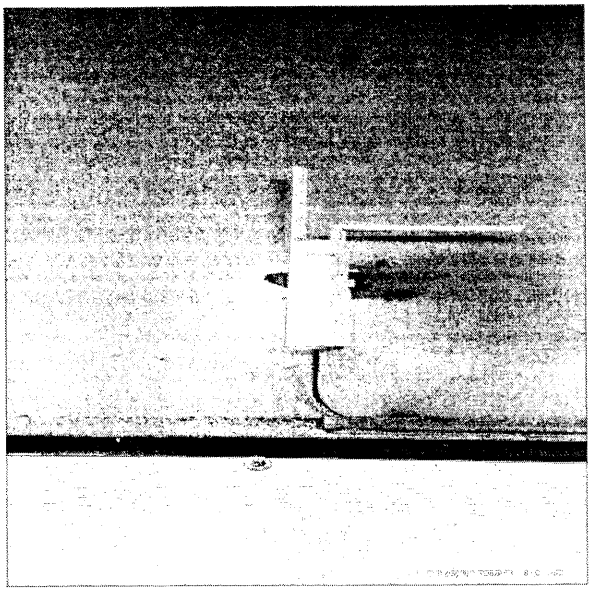


Sobre el espacio de disco del servidor Orfeo, en dialogo con la ingeniera Nancy Álvarez ya se escaló la solicitud de compra al contratista. Se está en espera de la entrega de disco duro.

6. Las demás asignadas por el supervisor de acuerdo con el objeto de contrato.

Se hace visita técnica al colegio integrado sede Uriel armando bravo para la validación de la instalación de los dos radios enlaces ac1200 acordados para el mejoramiento en la calidad del servicio de internet de la institución.





Lo anterior para efectos de pago.

Atentamente,

JOHN JAIRO SANCHEZ SOSA
Contratista

VoBo Supervisor